Научная статья

DOI: 10.15593/2224-9397/2023.3.06
УДК 004.056

З.А. Ахмарова, А.И. Заитов, А.И. Тур

Пермский национальный исследовательский политехнический университет,
Пермь, Российская Федерация

МОДЕЛЬ ОЦЕНКИ УГРОЗ ДЛЯ СИСТЕМ УМНОГО ДОМА

Домашняя автоматизация в современных условиях представляет собой чрезвычайно гибкую систему, которую пользователь конструирует и настраивает самостоятельно в зависимости от собственных потребностей. Однако неумелое использование подобных систем может стать источником большого количества угроз. Как правило, рядовому пользователю достаточно проблематично оценить риски и угрозы, связанные с использованием умного дома, а нанимать специалистов для решения подобных задач достаточно затратно. На текущий момент нет готовой модели оценки угроз, предназначенной для бытовых систем домашней автоматизации, что является серьёзным барьером для людей, старающихся разобраться в данном вопросе самостоятельно. **Цель исследования:** разработка авторской модели оценки угроз систем умного дома и методики её использования. Результатом работы является приложение – экспертная система, способная дать совет пользователю по мерам обеспечения безопасности его средств автоматизации. **Результаты**: в статье представлен алгоритм оценки угроз умного дома, предложены вариант актуальных угроз для систем умного дома бытового назначения и модель оценки угроз, а также вариант реализации приложения для пользователя домашней системы автоматизации, выполняющего роль помощника в настройке безопасности системы. Полученные результаты направлены на решение научно-практической задачи по упрощению и оптимизации процесса оценки уровня защищённости системы умного дома. Предложенная модель сформулирована для обобщённого случая, но может быть дополнена и модифицирована для конкретного случая эксплуатации системы домашней автоматизации.

Ключевые слова: система умного дома, информационная безопасность.

Z.A. Akhmarova, A.I. Zaitov, A.I. Tur

Perm National Research Polytechnic University, Perm, Russian Federation

THREAT ASSESSMENT MODEL FOR SMART HOME SYSTEMS

Home automation in modern conditions is an extremely flexible system that the user designs and configures independently, depending on their own needs. However, the inept use of such systems can become a source of a large number of threats. As a rule, it is rather problematic for an ordinary user to assess the risks and threats associated with the use of a smart house, and hiring specialists to solve such problems is quite costly. At the moment there is no ready-made threat assessment model designed for home automation systems, which is a serious barrier for people trying to understand this issue on their own. **The purpose** of this work is to development of an author's model for assessing threats to smart house systems and methods for its use. The result of the work is an expert system

capable of giving advice to the user on measures to ensure the security of his automation tools. **Results:** The paper presents an algorithm for evaluating smart home threats, proposes a variant of current threats for home smart home systems, a threat assessment model, and also proposes an application implementation option for a user of a home automation system that acts as an assistant in setting up system security. This is aimed at solving the scientific and practical problem of simplifying and optimizing the process of assessing the level of security of a smart home system. The proposed model is formulated for a generalized case, but can be supplemented and modified for a specific case of operating a home automation system.

Keywords: smart home system, information security.

Введение

Сегодня процесс автоматизации повсеместно внедряется в жизнь человека, в том числе и в отношении обычных бытовых задач. Однако при неумелом использовании автоматизация (в текущем её состоянии) может стать источником достаточно большого количества угроз. Благодаря инструкциям производителя пользователь вполне способен самостоятельно обеспечить правильную настройку функционала устройств автоматизации. Но, в условиях современных киберугроз в данный процесс может вмешиваться злоумышленник. Как правило, оценить риски и угрозы, связанные с использованием умного дома в подобных условиях, рядовому пользователю достаточно проблематично. Целью данной работы является разработка авторской модели оценки угроз умного дома и методики её использования для выявления слабых мест в сфере информационной безопасности. Результатом работы является приложение – экспертная система, способная дать рекомендации пользователю по мерам безопасности его средств автоматизации.

Интернет вещей – это вычислительная сеть физических объектов, оснащенных встроенными технологиями сбора и передачи информации в совокупности с устройствами и технологиями хранения и обработки информации. Домашняя автоматизация (home automation), или по-другому умный дом (smart house), рассматривается как частный случай интернета вещей. По своей сути это система домашних устройств, способных выполнять действия и решать определённые повседневные задачи без участия человека. Домашняя автоматизация включает в себя доступные через Интернет домашние устройства, в то время как интернет вещей включает любые связанные через Интернет устройства в принципе.

Домашняя автоматизация в современных условиях – чрезвычайно гибкая система, которую пользователь конструирует и настраивает самостоятельно в зависимости от собственных потребностей. Чаще всего

сегодня она представляет собой агломерацию устройств, способных принимать управляющие сигналы от центрального хаба, занимающегося получением и обработкой команд от человека.

На данный момент не существует единого чётко сформулированного подхода к оценке угроз умного дома. Существуют рекомендации ФСТЭК России и достаточно большой ряд моделей, которые их используют [1–3]. Однако рекомендации являются достаточно сложными для понимания человеком без опыта в сфере информационной безопасности, а модели преимущественно тяготеют к промышленным и распределённым вариантам интернета вещей. В данной статье предлагается упрощённая модель, которая опирается на актуальные для бытового уровня угрозы и может быть использована обычным пользователем, не обладающим специальными знаниями.

1. Основные элементы умного дома

Популярными примерами систем умного дома являются «умные колонки» – микрокомпьютер с интегрированным голосовым помощником, оснащённый человеко-машинным интерфейсом (микрофон и динамик, сенсорный экран, кнопки и т.д.) и средствами связи с другими умными устройствами (передатчиками Bluetooth, Wi-Fi, Zigbee и пр.). Безопасность подобных систем зависит от 2 основных факторов: безопасность канала передачи информации между хабом и конечными устройствами и безопасность человеко-машинного интерфейса.

В целом, вопросы безопасности передачи информации условно можно разделить: на безопасность канала передачи информации (насколько легко злоумышленник может подключиться к каналу); безопасность представления информации (сложность получения ценных сведений из перехваченного информационного трафика, обусловленная протоколом передачи информации, шифрованием и пр.) и безопасность передаваемой информации (отсутствие в передаваемой информации сведений, способных причинить вред владельцу устройства). На текущий момент абсолютное большинство предлагаемых на рынке продуктов имеет схожие решения данных задач:

– Wi-Fi с возможностью шифрования WPA (Wi-Fi Protected Access) или WPA2 (Wi-Fi Protected Access II) – передача объёмных данных (видеопоток от камеры, предоставление пользователю информации, получаемой из Интернета и пр.);

– Zigbee без шифрования – передача телеметрии от датчиков и отправка управляющих сигналов;

– в служебном трафике содержится минимальный объём данных, способных навредить обладателю устройства (персональные данные и прочее);

– при необходимости сообщить пользователю информацию, способную помочь злоумышленнику проникнуть в систему, предпочтительно применяется человеко-машинный интерфейс (автоматизированная авторизация устройства пользователя в системе с помощью специального звукового сигнала, издаваемого хабом или смартфоном [4, 5]).

Очевидно, что описанные выше способы не обеспечивают 100 % защиты от действий злоумышленника [6–11], но при надлежащей эксплуатации средств домашней автоматизации значительно затрудняют взлом подобной системы. При этом проблемы безопасности человеко-машинного интерфейса чаще всего остаются нерешенными. Иногда это обусловлено утверждением, что для использования человеко-машинного интерфейса требуется нахождение злоумышленника на территории умного дома (например, информация, отображаемая на дисплее) или непосредственно взаимодействие с хабом (например, кнопка или сенсорный экран). Однако наблюдается общая тенденция к переходу на бесконтактные способы взаимодействия с хабом посредствам голоса [12–14], звуков [5, 15–17], жестов [16, 18]. Подобные ситуации являются сложными с точки зрения реализации функций защиты и не менее опасными, чем рассмотренные ранее.

Например, существуют примеры инициализации хаба в домашней Wi-Fi-сети с помощью звукового сигнала, издаваемого другим устройством пользователя (смартфон, планшет и пр.). Устройство собирает данные о сети (ssid, пароль) и о профиле пользователя в приложении (логин, пароль), кодирует, модулирует звук и воспроизводит его динамиком (хаб с помощью микрофона распознаёт команду на подключение).

2. Модель оценки угроз

Учитывая вышеизложенное, предлагается авторская модель оценки угроз, актуальных для систем домашней автоматизации (таблица).

Угрозы разделены на две категории: кража информации пользователя (например, «Wi-Fi (с WPA) – кража данных пользователя») и внедрение злоумышленником в систему потенциально опасных уст-

ройств (например, «Wi-Fi (с WPA) – внедрение в систему» и «Звуковые сигналы для служебных команд»), поскольку по экспертной оценке, [1–3, 19–25] они являются схожими по принципу, но несут различные последствия (и, как следствие, требуют разных методов защиты). Угрозы, связанные с взаимодействием злоумышленника с человеко-машинными интерфейсами системы, дополнительно разделены по принципу возможности подачи управляющих команд умному дому.

Оценка угроз системы умного дома, характерных для домашнего использования

Наименование угрозы	Опасность атаки	Вероятность при доступе в помещение	Вероятность при нахождении вблизи помещения	Вероятность при нахождении вдали от помещения
Wi-Fi (с WPA) – кража данных пользователя	Высокая (3)	Средняя (2)	Средняя (2)	Низкая (1)
Wi-Fi (с WPA) – внедрение в систему	Средняя (2)	Средняя (2)	Средняя (2)	Низкая (1)
ZigBee – внедрение в систему	Высокая (3)	Высокая (3)	Высокая (3)	Низкая (1)
Bluetooth – кража данных пользователя	Высокая (3)	Высокая (3)	Средняя (2)	Низкая (1)
Bluetooth – внедрение в систему	Средняя (2)	Высокая (3)	Средняя (2)	Низкая (1)
Звуковые сигналы для служебных команд	Высокая (3)	Высокая (3)	Низкая (1)	Отсутствует (0)
Оптические сигналы для служебных команд	Высокая (3)	Высокая (3)	Высокая (3)	Низкая (1)
Контактный интерфейс для служебных команд	Высокая (3)	Высокая (3)	Отсутствует (0)	Отсутствует (0)
Звуковые сигналы для неслужебных команд	Средняя (2)	Высокая (3)	Низкая (1)	Отсутствует (0)
Оптические сигналы для неслужебных команд	Средняя (2)	Высокая (3)	Высокая (3)	Низкая (1)
Контактный интерфейс для неслужебных команд	Низкая (1)	Высокая (3)	Отсутствует (0)	Отсутствует (0)

К группе звуковых сигналов отнесены различные звуки, модулированные мелодии и речь человека (если система оснащена модулем распознавания речи). К группе оптических сигналов отнесены любые взаимодействия с хабом, требующие визуального контакта, – ИК сигналы, QR-коды (демонстрируемые любым способом), жесты пользователя (если система оснащена модулем распознавания визуальных образов).

Под контактным интерфейсом понимается человеко-машинный интерфейс, представленный кнопками, тумблерами, потенциометрами, сенсорными экранами и иными средствами ввода информации человеком, требующими прямого физического взаимодействия с пользователем.

Злоумышленник во всех случая считается компетентным для реализации атаки и обладающим базовыми средствами реализации, доступными обычному человеку. Вероятность реализации атаки рассчитывается, исходя из удалённости злоумышленника от центрального хаба умного дома. Под «доступом в помещение» понимается возможность злоумышленника контактировать с хабом физически. Под «нахождением вблизи» – возможность злоумышленника контактировать с хабом только дистанционно, но в зоне уверенного приёма сигналов (визуально – через окно помещения, аудиально – в пределах отчётливой слышимости спокойного человеческого голоса, в радиусе действия Wi-Fi/ZigBee/Bluetooth с уровнем сигнала не ниже среднего и т.д.).

Возможность злоумышленника отправлять управляющие сигналы (независимо от их вида) несёт большую опасность для системы, так как открывает неограниченные возможности по внедрению и получению данных. Остальные варианты рассмотренных угроз базируются на экспертной оценке, основанной на информации, передающейся указанным способом.

Протоколы ZigBee преимущественно используются только для обмена информацией и отправки управляющих сигналов устройствами умного дома. В данном случае обычно применяется система защиты, использующая ключи и временные метки, синхронизирующие устройства. Это означает, что злоумышленник, при достаточном количестве времени, может перехватить синхронизационную информацию и внедриться в систему как новое устройство, так и ещё один управляющий хаб (возможно только для отдельных систем умного дома). Поэтому данная угроза имеет статус высокой опасности.

Bluetooth используется достаточно редко (предпочтение производителей отдаётся Wi-Fi), но всё ещё применяется для сопряжения и передачи пользовательской информации между устройствами. Чаще всего такими устройствами являются внешние (дополнительные) колонки или контроллеры/пульты управления. Перехват подобной информации или внедрение в систему в виде дополнительного внешнего устройства несёт среднюю опасность, так как чаще всего не содержит информации конфиденциального характера или служебных данных системы, позволяющих злоумышленнику получить конфиденциальную информацию. Исключением является атака «человек посередине» (MITM, «man in the middle») на устройства, используемые для ведения телефонного разговора (беспроводная гарнитура, внешние колонки и т.д.) – для данных случаев опасность атаки оценивается как высокая.

Wi-Fi используется для схожих целей, как и Bluetooth, но имеет более высокую пропускную способность. Это позволяет передавать больший объём информации – большинство подключаемых устройств умного дома могут использовать Wi-Fi (смартфоны/планшеты/компьютеры, видеокамеры, телевизоры и пр.). Перехват подобного трафика несёт высокую опасность, так как содержит большой объём конфиденциальной информации пользователя умного дома. Поэтому использование такого подключения без защиты (WPA и более новые варианты) и циркуляция такого трафика в открытом виде крайне нежелательны. В то же время использование Wi-Fi для внедрения в систему имеет среднюю опасность, так как не позволит злоумышленнику получать полный объём информации из-за средств защиты и ограничений, используемых хабами умного дома (они включены по умолчанию в подобных устройствах, если пользователь целенаправленно их не выключил). Кроме того, такое подключение чаще всего требует подтверждения пользователя, что значительно осложняет незаметное подключение злоумышленником (обычный перехват трафика является незаметным для пользователя и не может быть заблокирован в силу природы среды передачи сигнала).

Сигналы, циркулирующие в системе умного дома, не несущие управляющих команд (независимо от их вида), чаще всего не содержат опасный объём конфиденциальной информации. Исключением являются системы, использующие модулированные звуковые сигналы и QR-коды, применяемые для автоматизированной авторизации (ssid

и пароль Wi-Fi сети, логин и пароль для авторизации в системе) – эти данные могут быть подслушаны злоумышленником и использованы для подключения своего устройства. Однако такие системы являются достаточно сложными в реализации для злоумышленника, находящегося вне помещения, и не дают значительных возможностей при использовании.

Для интуитивно понятного использования предложенной модели оценки угроз умного дома обычным пользователем реализовано экспертное приложение. Алгоритм его работы представлен на рис. 1.

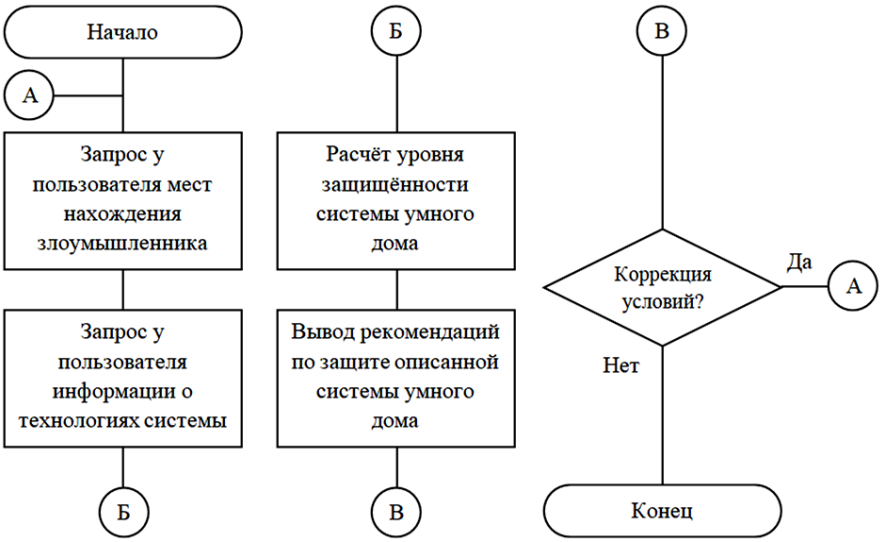

Рис. 1. Схема алгоритма работы экспертной системы

Для расчёта уровня защищённости системы умного дома применяется следующая формула:

$$F = \sum(D_n \cdot P_n) \cdot A_n, \quad (1)$$

где D_n – коэффициент опасности атаки, P_n – коэффициент вероятности реализации атаки злоумышленником, A_n – наличие в системе интерфейса/среды передачи сигнала, используемых для атаки. Чем ниже результирующее значение функции F, тем более безопасно использование системы умного дома в обозначенных условиях.

Коэффициент опасности атаки соответствует данным таблицы и рассчитывается как «высокий» – 3, «средний» – 2, «низкий» – 1. Коэффициент вероятности реализации атаки злоумышленником: «высокая» – 3, «средняя» – 2, «низкая» – 1, «отсутствует» – 0. В случае,

если в системе отсутствует интерфейс/среда передачи сигнала, используемый для атаки, то коэффициент наличия равен 0, иначе – 1. Предложенный вариант экспертной системы содержит базовые угрозы, которые могут быть дополнены в случае выявления иных актуальных угроз. В случае изменения вероятности реализации или опасности атаки изменения в системе потребуются только изменения соответствующих коэффициентов.

3. Экспертное приложение оценки угроз умного дома

На рис. 2 представлен пример графического интерфейса разработанного приложения «Экспертная система безопасности умного дома».

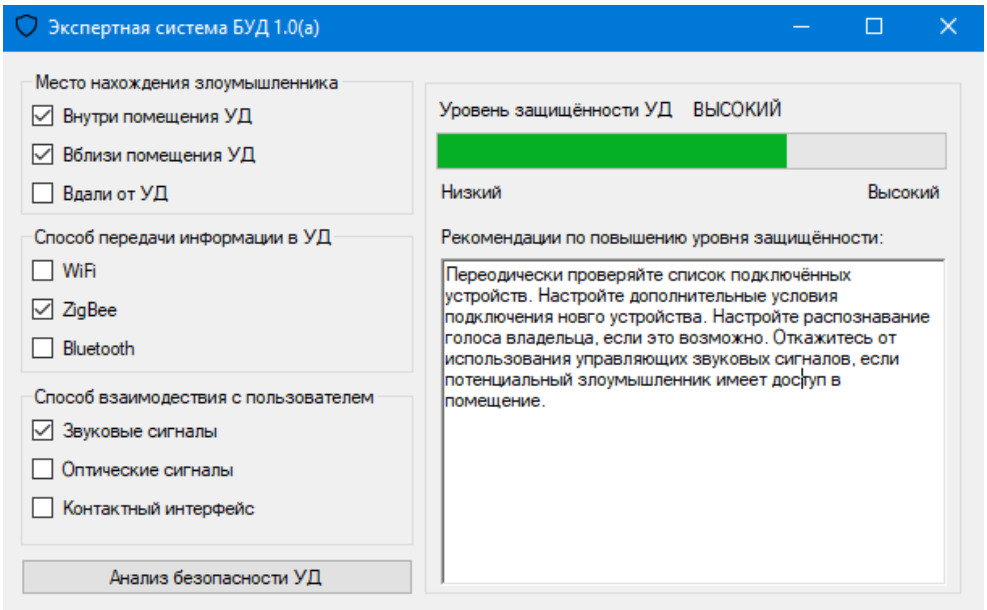

Рис. 2. Экран расчёта Уровня защищённости умного дома

Согласно алгоритму (см. рис. 1), система опрашивает пользователя о защищаемой системе умного дома, используя значения таблицы (представленные в численном виде), проводит анализ по формуле (1) и выносит заключение об уровне защищённости умного дома, предлагая пользователю рекомендации по повышению безопасности.

Данный пример выполнен с использованием фреймворка .NET, однако, может быть легко перенесён на любой другой фреймворк для повышения удобства взаимодействия пользователя с экспертным приложением.

Благодаря модульной конструкции предложенное приложение может быть легко модифицировано (добавление новых актуальных угроз, редактирование числовых весов угроз, вынесение в базу дополнительных рекомендаций для пользователя) для тех или иных условий использования. Для этого необходимо внести изменения во внешний файл, представляющий собой интерпретацию таблицы.

Преимуществом такого подхода является возможность быстрого редактирования показателей опасности и вероятности реализации атак без необходимости переустановки или исправления кода самой программы.

Файл модели оценки угроз может распространяться как поставщиком решений для умного дома, так и авторитетными специалистами по защите информации, способными оперативно актуализировать данные о существующих угрозах.

После запуска приложения файл модели оценки угроз считывается и преобразуется в числовые коэффициенты для переменных, участвующих в расчёте, по выражению (1).

Также имеется дополнительный файл, хранящий в себе текстовое описание рекомендаций по повышению уровня защищённости. Преимущественно данные рекомендации носят обобщённый характер и достаточно универсальны. Поэтому необходимости обновлять его также часто, как модель оценки угроз, нет. Однако такая возможность имеется (выполняется аналогично вышеописанному случаю).

После расчёта уровня защищённости приложение с помощью специальных численных флагов обращается к файлу рекомендаций и загружает те, что в большей степени подходят для описанной пользователем системы.

Заключение

Предложенная оригинальная модель оценки угроз умного дома позволяет в упрощённой форме в достаточной степени оценить реально существующее состояние информационной защищённости системы домашней автоматизации.

Благодаря разработанному приложению оценка является простой и доступной обычному пользователю. Однако при необходимости, для повышения точности оценки и актуализации угроз, приложение ввиду его модульной структуры может быть расширено и дополнено.

С практической точки зрения предложенный подход направлен на упрощение оценки уровня защищённости систем умного дома. Это позволит снизить нагрузку на специалистов в области защиты информации, а также будет способствовать популяризации принципов информационной безопасности среди обычных пользователей.

Сама модель является производной от рекомендаций ФСТЭК России. Вариант, представленный в данной статье, с научной точки зрения направлен на оптимизацию работы специалиста по оценке уровня защищённости информационной системы. Достигается это благодаря выбору наиболее актуальных угроз именно для систем умного дома и корректировке вероятности реализации атаки злоумышленника (для примера выбран профиль злоумышленника, обладающего средними возможностями: умеет применять готовые решения и продукты для проведения атак, не знаком с сетевой структурой цели и со средней мотивацией (кража информации и персональных данных для дальнейшего извлечения прибыли)).

Библиографический список

1. Формализованная модель информационной безопасности системы «Умный дом» / Н.А. Овчинников, К.В. Мисюрина, М.Н. Рудикова, Е.А. Максимова // Апробация. – 2016. – № 1 (40). – С. 49–51.

2. Сатаев Д.Г. Угрозы информационной безопасности системы «Умный дом» // Электронный научный журнал. – 2019. – № 6 (26). – С. 24–28.

3. Бондарева А.Д. Модель нарушителя информационной безопасности в системах типа «Умный дом» // Альманах научных работ молодых ученых университета ИТМО: XLVII науч. и учебно-метод. конф. ун-та ИТМО; Санкт-Петербург, 30 января – 02 февраля 2018 г. Т. 1. – СПб.: Изд-во Нац. исслед. ун-та ИТМО, 2018. – С. 94–98.

4. Мелимов А.А. Угрозы информационной безопасности в автоматизированных системах управления типа «Умный дом» // Безопасность городской среды: материалы IV Междунар. науч.-практ. конф.; Омск, 16–18 ноября 2016 г. – Омск: Изд-во Омск. гос. техн. ун-та, 2017. – С. 365–367.

5. Филиппов С.А., Саломасова И.А. Применимость «умных» колонок в системах типа «Умный» дом // Теория. Практика. Инновации. – 2019. – № 4 (40). – С. 29–37.

6. Крупник С.А. Реверс инжиниринг протокола активации Яндекс.Станции [Электронный ресурс]. – URL: https://habr.com/ru/articles/469435/ (дата обращения: 14.05.2023).

7. Белорусов Д.И., Корешков М.С. WIFI-сети и угрозы информационной безопасности // Специальная техника. – 2009. – № 6. – С. 2–6.

8. Белетова Д.У., Молчанов А.Н. Использование стандарта IEEE 802.1x для защиты от НСД // Электронный журнал: наука, техника и образование. – 2017. – № 1 (10). – С. 6–15.

9. Белова Т.С., Клочко О.С. Безопасность данных, передаваемых по сети Wi-Fi // Электронный журнал: наука, техника и образование. – 2016. – № 4 (9). – С. 54–61.

10. Грязин Д.С., Данилова А.А. Безопасность повышенного уровня в сетях Zigbee // Перспективы развития информационных технологий. – 2014. – № 17. – С. 90–94.

11. Лысов Д.А., Филин А.А., Чайко А.А. Организация безопасности при использовании протокола беспроводной передачи данных Zigbee // Моя профессиональная карьера. – 2020. – Т. 3, № 11. – С. 15–21.

12. Десницкий В.А., Котенко И.В. Моделирование и анализ инцидентов безопасности мобильной коммуникационной самоорганизующейся сети на базе протокола ZigBee // Материалы Междунар. конф. по мягким вычислениям и измерениям. – 2017. – Т. 2. – С. 39–42.

13. Малых Д.А., Кириллова Ю.С. Система управления устройствами «умного дома» с использованием голосовых команд // Молодой ученый. – 2017. – № 19 (153). – С. 60–64.

14. Еременко В.О., Молодяков С.А. Управление умным домом с помощью диалоговых команд голосового управления // Современные технологии в теории и практике программирования: сб. материалов конф.; Санкт-Петербург, 23 апреля 2020 г. / Санкт-Петербург. политехн. ун-т Петра Великого; Dell Technologies; EPAM Systems. – СПб.: Политех-пресс, 2020. – С. 17–18.

15. Ефремов В.М. К вопросу использования голосовых помощников в умном доме // Лига молодых учёных: сб. ст. междунар. науч.-практ. конф.; Пенза, 27 марта 2023 г. – Пенза: Наука и просвещение (ИП Гуляев Г.Ю.), 2023. – С. 27–29.

16. Св-во о гос. регистр. программы для ЭВМ № 2020661551 Рос. Федерация. Голосовой помощник секретарь: № 2020660398; заявл. 10.09.2020; опубл. 24.09.2020; заявит. ООО «Ай-Сис Лабс».

17. Халиуллин А.В. Навык Алисы на serverless в Yandex.Cloud [Электронный ресурс]. – URL: https://habr.com/ru/articles/570470/ (дата обращения: 14.05.2023).

18. Клюев Л.В. Как устроена Алиса. Лекция Яндекса [Электронный ресурс]. – URL: https://habr.com/ru/companies/yandex/articles/349372/ (дата обращения: 14.05.2023).

19. Св-во о гос. регистр. программы для ЭВМ № 2022610973 Рос. Федерация. Модуль NeoMe для программного продукта «Умное зеркало» ArtikMe PRO: № 2021682362; заявл. 30.12.2021; опубл. 18.01.2022 / Д.О. Андреев, И.И. Григорьев, Р.М. Исмагилов [и др.]; заявит. ООО «Стендап инновации».

20. Агаджанов М.В. Проект Reflecty: зеркало как часть умного дома [Электронный ресурс]. – URL: https://habr.com/ru/articles/392119/ (дата обращения: 14.05.2023).

21. Alexandrov V.A., Desnitsky V.A., Chaly D.Y. Design and security analysis of a fragment of internet of things telecommunication system // Automatic control and computer sciences. – 2019. – Vol. 53, № 7. – P. 851–856. DOI: 10.3103/S0146411619070241

22. Kushnir I., Malykhin O. Functional and methodological subsystems of content transformations of operating systems for enterprises-stakeholders in the «smart House» projects // International Independent Scientific Journal. – 2022. – № 41. – P. 10–15. DOI: 10.5281/zenodo.6980262

23. Dokhnyak B., Vysotska V. Intelligent smart home system using amazon alexa tools // CEUR Workshop Proceedings: 3, Lviv-Shatsk, 05–06 июня 2021 г. – Lviv-Shatsk, 2021. – P. 441–464.

24. Building a speech recognition system with privacy identification information based on Google Voice for social robots / P.C. Lin, B. Yankson, V. Chauhan, M. Tsukada // The Journal of Supercomputing. – 2022. – Vol. 78. – P. 15060–15088. DOI: 10.1007/s11227-022-04487-3

25. Security management in smart home environment / L.M. Gladence, V.M. Anu, S. Revathy, P. Jeyanthi // Soft Computing. – 2021. DOI: 10.1007/s00500-021-06054-z

References

1. Ovchinnikov N.A., Misiurina K.V., Rudikova M.N., Maksimova E.A. Formalizovannaia model' informatsionnoi bezopasnosti sistemy “Umnyi dom” [Formalized model of information security of the "Smart House" system]. *Aprobatsiia*, 2016, no. 1 (40), pp. 49-51.

2. Sataev D.G. Ugrozy informatsionnoi bezopasnosti sistemy “Umnyi dom” [Threats to information security of the "Smart Home" system]. *Elektronnyi nauchnyi zhurnal*, 2019, no. 6 (26), pp. 24-28.

3. Bondareva A.D. Model' narushitelia informatsionnoi bezopasnosti v sistemakh tipa “Umnyi dom” [Information security violator model in "Smart home" type systems]. *Al'manakh nauchnykh rabot molodykh uchenykh universiteta informatsionnykh tekhnologii, mekhaniki i optiki. XLVII nauchnaia i uchebno-metodicheskaia konferentsiia universiteta informatsionnykh tekhnologii, mekhaniki i optiki; Saint Petersburg, 30 January - 02 February 2018*. Saint Petersburg: Sankt-Peterburgskii natsional"nyi issledovatel"skii universitet informatsionnykh tekhnologii, mekhaniki i optiki, 2018, vol. 1, pp. 94-98.

4. Melimov A.A. Ugrozy informatsionnoi bezopasnosti v avtomatizirovannykh sistemakh upravleniia tipa “Umnyi dom” [Threats to information security in automated control systems such as “Smart House”]. *Bezopasnost' gorodskoi sredy. Materialy IV Mezhdunarodnoi nauchno-prakticheskoi konferentsii; Omsk, 16-18 November 2016*. Omsk: Omskii gosudarstvennyi tekhnicheskii universitet, 2017, pp. 365-367.

5. Filippov S.A., Salomasova I.A. Primenimost' “umnykh” kolonok v sistemakh tipa “Umnyi” dom [Applicability of “smart” speakers in systems such as “Smart” home]. *Teoriia. Praktika. Innovatsii*, 2019, no. 4 (40), pp. 29-37.

6. Krupnik S.A. Revers inzhiniring protokola aktivatsii Iandeks.Stantsii [Reverse engineering of the Yandex.Station activation protocol], available at: https://habr.com/ru/articles/469435/ (accessed 14 May 2023).

7. Belorusov D.I., Koreshkov M.S. Wi-Fi-seti i ugrozy informatsionnoi bezopasnosti Wi-Fi networks and information security threats]. *Spetsial'naia tekhnika*, 2009, no. 6, pp. 2-6.

8. Beletova D.U., Molchanov A.N. Ispol'zovanie standarta IEEE 802.1x dlia zashchity ot NSD [Using the IEEE 802.1x standard for tamper protection]. *Elektronnyi zhurnal: nauka, tekhnika i obrazovanie*, 2017, no. 1 (10), pp. 6-15.

9. Belova T.S., Klochko O.S. Bezopasnost' dannykh, peredavaemykh po seti Wi-Fi [Security of data transmitted over the Wi-Fi network]. *Elektronnyi zhurnal: nauka, tekhnika i obrazovanie*, 2016, no. 4 (9), pp. 54-61.

10. Griazin D.S., Danilova A.A. Bezopasnost' povyshennogo urovnia v setiakh Zigbee [Advanced Security in ZIgbee Networks]. *Perspektivy razvitiia informatsionnykh tekhnologii*, 2014, no. 17, pp. 90-94.

11. Lysov D.A., Filin A.A., Chaiko A.A. Organizatsiia bezopasnosti pri ispol'zovanii protokola besprovodnoi peredachi dannykh Zigbee [Organization of security when using the zigbee wireless data transfer protocol]. *Moia professional'naia kar'era*, 2020, vol. 3, no. 11, pp. 15-21.

12. Desnitskii V.A., Kotenko I.V. Modelirovanie i analiz intsidentov bezopasnosti mobil'noi kommunikatsionnoi samoorganizuiushcheisia seti na baze protokola ZigBee [Modeling and analysis of security incidents of a mobile communication self-organizing network based on the ZigBee protocol]. *Materialy Mezhdunarodnoi konferentsii po miagkim vychisleniiam i izmereniiam*, 2017, vol. 2, pp. 39-42.

13. Malykh D.A., Kirillova Iu.S. Sistema upravleniia ustroistvami "umnogo doma" s ispol'zovaniem golosovykh komand [Smart home device control system using voice commands]. *Molodoi uchenyi*, 2017, no. 19 (153), pp. 60-64.

14. Eremenko V.O., Molodiakov S.A. Upravlenie umnym domom s pomoshch'iu dialogovykh komand golosovogo upravleniia [Smart home control with voice commands]. *Sovremennye tekhnologii v teorii i praktike programmirovaniia. Sbornik materialov konferentsii; Saint Petersburg, 23 April 2020. Sankt-Peterburgskii politekhnicheskii universitet Petra Velikogo; Dell Technologies; EPAM Systems*. Saint Petersburg: Politekh-press, 2020, pp. 17-18.

15. Efremov V.M. K voprosu ispol'zovaniia golosovykh pomoshnikov v umnom dome [On the issue of using voice assistants in a smart home]. *Liga molodykh uchenykh. Sbornik statei mezhdunarodnoi nauchno-prakticheskoi konferentsii; Penza, 27 March 2023*. Penza: Nauka i prosveshchenie (IP Guliaev G.Iu.), 2023, pp. 27-29.

16. Golosovoi pomoshchnik sekretar' [Voice assistant secretary]. Svidetel'stvo o gosudarstvennoi registratsii programmy dlia EVM no. 2020661551 (2020).

17. Khaliullin A.V. Navyk Alisy na serverless v Yandex.Cloud [Alice's skill on serverless in Yandex.Cloud], available at: https://habr.com/ru/articles/570470/ (accessed 14 May 2023).

18. Kliuev L.V. Kak ustroena Alisa. Lektsiia Iandeksa [How is Alice. Yandex lecture], available at: https://habr.com/ru/companies/yandex/articles/349372/ (accessed 14 May 2023).

19. Andreev D.O., Grigor'ev I.I., Ismagilov R.M. [et al.] Modul' NeoMe dlia programmnogo produkta «Umnoe zerkalo» ArtikMe PRO

[NeoMe module for the ArtikMe PRO Smart Mirror software product]. Svidetel'stvo o gosudarstvennoi registratsii programmy dlia EVM no. 2022610973 (2022).

20. Agadzhanov M.V. Proekt Reflecty: zerkalo kak chast' umnogo doma [Reflecty project: a mirror as part of a smart home], available at: https://habr.com/ru/articles/392119/ (accessed 14 May 2023).

21. Alexandrov V.A., Desnitsky V.A., Chaly D.Y. Design and security analysis of a fragment of internet of things telecommunication system. *Automatic control and computer sciences*, 2019, vol. 53, no. 7, pp. 851-856. DOI: 10.3103/S0146411619070241

22. Kushnir I., Malykhin O. Functional and methodological subsystems of content transformations of operating systems for enterprises-stakeholders in the "smart House" projects. *International Independent Scientific Journal*, 2022, no. 41, pp. 10-15. DOI: 10.5281/zenodo.6980262

23. Dokhnyak B., Vysotska V. Intelligent smart home system using amazon alexa tools // *CEUR Workshop Proceedings: 3, Lviv-Shatsk, 05-06 June 2021*. Lviv-Shatsk, 2021, pp. 441-464.

24. Lin P.C., Yankson B., Chauhan V., Tsukada M. Building a speech recognition system with privacy identification information based on Google Voice for social robots. *The Journal of Supercomputing*, 2022, vol. 78, pp. 15060-15088. DOI: 10.1007/s11227-022-04487-3

25. Gladence L.M., Anu V.M., Revathy S., Jeyanthi P. Security management in smart home environment. *Soft Computing*, 2021. DOI: 10.1007/s00500-021-06054-z

Сведения об авторах

Ахмарова Зульфия Айдаровна (Пермь, Российская Федерация) – студентка Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: ZAKhmarova@bK.ru).

Заитов Айрат Ильшатович (Пермь, Российская Федерация) – студент Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: Zaitov.airat2001@yandex.ru).

Тур Александр Игоревич (Пермь, Российская Федерация) – кандидат технических наук, доцент кафедры «Автоматика и телемехани-

ка» Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: tur.aleksandr93@mail.ru).

About the authors

Zul'fiya A. Akhmarova (Perm, Russian Federation) – Student Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: ZAKhmarova@bK.ru).

Ayrat I. Zaitov (Perm, Russian Federation) – Student Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: Zaitov.airat2001@yandex.ru).

Aleksandr I. Tur (Tomsk, Russian Federation) – Ph. D. in Technical Sciences, Department of Automation and telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: tur.aleksandr93@mail.ru).

Поступила: 15.05.2023. Одобрена: 20.08.2023. Принята к публикации:01.10.2023.

Финансирование. Исследование не имело спонсорской поддержки.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов по отношению к статье.

Вклад авторов. Все авторы сделали равноценный вклад в подготовку статьи.

Просьба ссылаться на эту статью в русскоязычных источниках следующим образом:

Ахмарова, З.А. Модель оценки угроз для систем умного дома / З.А. Ахмарова, А.И. Заитов, А.И. Тур // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2023. – № 47. – С. 105–121. DOI: 10.15593/2224-9397/2023.3.06

Please cite this article in English as:

Akhmarova Z.A., Zaitov A.I., Tur A.I. Threat assessment model for smart home systems. *Perm National Research Polytechnic University Bulletin. Electrotechnics, information technologies, control systems*, 2023, no. 47, pp. 105-121. DOI: 10.15593/2224-9397/2023.3.06